UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/665,826	09/20/2000	Luke E. Girard	042390.P8184	8683

7590 05/19/2004

John Travis
Blakely Sokoloff Taylor & Zafman LLP
12400 Wilshire Boulevard 7th Floor
Los Angeles, CA 90025

EXAMINER	
REVAK, CHRISTOPHER A	

ART UNIT	PAPER NUMBER
2131	3

DATE MAILED: 05/19/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/665,826	GIRARD ET AL.	
	Examiner	Art Unit	
	Christopher A. Revak	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *April 7, 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 2.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Information Disclosure Statement

1. The information disclosure statement (IDS) submitted on April 7, 2003 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 4 and 9 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

4. Claims 4 and 9 both recite the limitation "the security mode" in line 2. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States

only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-22 are rejected under 35 U.S.C. 102(e) as being anticipated by Schreiber et al, U.S. Patent 6,298,446.

As per claim 1, it is disclosed by Schreiber et al of a method comprising receiving data in a video buffer (presentation buffer) that is associated with a web browser plug-in (presentation controller) that allows for displaying the image (col. 3, lines 2-3,27-33). A request is received from a client computer (requestor) for an original layout page containing references to digital images and the original layout page is parsed and a modified layout page is presented to the user by using substitute data and not delivering the original layout page containing the digital images to the requestor (col. 3, lines 39-47). It is interpreted by the examiner that the data is then read by the user's computer since it is to be displayed to a user by means of the web browser plug-in (presentation controller)(col. 3, lines 27-33,39-47). Access is blocked to the pixel data of the digital image in the video buffer (presentation buffer)(col. 4, lines 37-42 and col. 18, lines 65-68). The substitute pixel data replaces (by deleting) the protected pixel data (col. 19, line 56).

As per claim 2, it is recited by Schreiber et al of a mode where protection applies on an image by image basis (col. 9, lines 1-4). The teachings disclose of the use of a video buffer (presentation buffer)(col. 3, lines 30-33) and it is inherent that a frame buffer is used since frame buffers hold the contents of a single screen image. The teachings also recite that the web browser plug-in (presentation controller) views

images and is interpreted as being a graphics controller since the graphics are displayed on a video monitor (col. 6, lines 42-45).

As per claim 3, Schreiber et al teaches of placing the web browser plug-in (presentation controller) in a protection (security) mode (col. 3, lines 27-33 and col. 8, lines 36-43).

As per claim 4, Schreiber et al discloses of placing the web browser plug-in (presentation controller) in a protection (security) mode (col. 3, lines 27-33 and col. 8, lines 36-43). It can be selected that the images be changed to unprotected (col. 9, lines 5-8) which is interpreted by the examiner as taking the presentation controller out of the protection (security) mode.

As per claim 5, Schreiber et al teaches of a modified layout page is presented to the user by using substitute data (delivering data other than the data requested) and not delivering the original layout page containing the digital images to the requestor (col. 3, lines 39-47).

As per claim 6, it is disclosed by Schreiber et al of receiving data in a video buffer (presentation buffer) that is associated with a web browser plug-in (presentation controller) that allows for displaying the image that is requested (and executed) by a command processor (col. 3, lines 2-3,27-33 and column 4, lines 55-59). It is it inherent that the web browser (instructions) are stored on a machine readable medium since it is necessary for the processor to read, interpret, and execute the instructions for the browser in order for it to function properly. A request is received from a client computer (requestor) for an original layout page containing references to digital images and the

original layout page is parsed and a modified layout page is presented to the user by using substitute data and not delivering the original layout page containing the digital images to the requestor (col. 3, lines 39-47). It is interpreted by the examiner that the data is then read by the user's computer since it is to be displayed to a user by means of the web browser plug-in (presentation controller)(col. 3, lines 27-33,39-47). Access is blocked to the pixel data of the digital image in the video buffer (presentation buffer)(col. 4, lines 37-42 and col. 18, lines 65-68). The substitute pixel data replaces (by deleting) the protected pixel data (col. 19, line 56).

As per claim 7, it is recited by Schreiber et al of a mode where protection applies on an image by image basis (col. 9, lines 1-4). The teachings disclose of the use of a video buffer (presentation buffer)(col. 3, lines 30-33) and it is inherent that a frame buffer is used since frame buffers hold the contents of a single screen image. The teachings also recite that the web browser plug-in (presentation controller) views images and is interpreted as being a graphics controller since the graphics are displayed on a video monitor (col. 6, lines 42-45).

As per claim 8, Schreiber et al teaches of placing the web browser plug-in (presentation controller) in a protection (security) mode (col. 3, lines 27-33 and col. 8, lines 36-43).

As per claim 9, Schreiber et al discloses of placing the web browser plug-in (presentation controller) in a protection (security) mode (col. 3, lines 27-33 and col. 8, lines 36-43). It can be selected that the images be changed to unprotected (col. 9, lines

5-8) which is interpreted by the examiner as taking the presentation controller out of the protection (security) mode.

As per claim 10, Schreiber et al teaches of a modified layout page is presented to the user by using substitute data (delivering data other than the data requested) and not delivering the original layout page containing the digital images to the requestor (col. 3, lines 39-47).

As per claim 11, it is disclosed by Schreiber et al of a system comprising receiving data in a video buffer (presentation buffer) that is associated with a web browser plug-in (presentation controller) that allows for displaying the image (col. 3, lines 27-33 and col. 4, lines 54-55). Contained within the system is a command processor (command handler) that processes commands made through the web browser to download information from web pages (located at a specific address)(col. 4, lines 54-60 and col. 6, lines 36-51). A web browser (additionally acting as a data handler) requests for data and pass the data to the video buffer (presentation buffer)(col. 3, lines 30-47). It is interpreted by the examiner that the web browser monitors for user requests to access data on the web pages (col. 6, lines 42-51). A request interceptor (security violation detector) detects requests by a client computer (requestor) to the protected data in the video buffer (presentation buffer)(col. 3, lines 39-47 and col. 6, lines 66-67). It is interpreted by the examiner that the data is then read by the user's computer since it is to be displayed to a user by means of the web browser plug-in (presentation controller)(col. 3, lines 27-33,39-47). A request blocker (data protector) that is coupled to the web browser (data handler) to prevent the

providing of the protected data whereby the substitute pixel data replaces (by not providing) the protected pixel data (col. 4, lines 59-60 and col. 19, line 56). Access is blocked to the pixel data of the digital image in the video buffer (presentation buffer)(col. 4, lines 37-42 and col. 18, lines 65-68).

As per claim 12, Schreiber et al teaches of a request blocker (data protector) that is coupled to the web browser (data handler) to prevent the providing of the protected data whereby the substitute pixel data replaces (purges) the protected pixel data (col. 4, lines 59-60 and col. 19, line 56). Data is received in a video buffer (presentation buffer) that is associated with a web browser plug-in (presentation controller) that allows for displaying the image (col. 3, lines 27-33 and col. 4, lines 54-55). It is interpreted by the examiner that the data is then read by the user's computer since it is to be displayed to a user by means of the web browser plug-in (presentation controller)(col. 3, lines 27-33,39-47).

As per claim 13, it is recited by Schreiber et al of a mode where protection applies on an image by image basis (col. 9, lines 1-4). The teachings disclose of the use of a video buffer (presentation buffer)(col. 3, lines 30-33) and it is inherent that a frame buffer is used since frame buffers hold the contents of a single screen image. The teachings also recite that the web browser plug-in (presentation controller) views images and is interpreted as being a graphics controller since the graphics are displayed on a video monitor (col. 6, lines 42-45).

As per claim 14, Schreiber et al discloses of placing the web browser plug-in (presentation controller) in a protection (security) mode (col. 3, lines 27-33 and col. 8,

lines 36-43). It can be selected that the images be changed to unprotected (col. 9, lines 5-8) which is interpreted by the examiner as placing the presentation controller in a by-pass mode.

As per claim 15, Schreiber et al teaches of a request blocker (data protector) that is coupled to the web browser (data handler) to prevent the providing of the protected data whereby the substitute pixel data replaces (purges) the protected pixel data (col. 4, lines 59-60 and col. 19, line 56). Data is received in a video buffer (presentation buffer) that is associated with a web browser plug-in (presentation controller) that allows for displaying the image (col. 3, lines 27-33 and col. 4, lines 54-55). It is interpreted by the examiner that the data is then read by the user's computer since it is to be displayed to a user by means of the web browser plug-in (presentation controller)(col. 3, lines 27-33,39-47). It is additionally recited by Schreiber et al of placing the web browser plug-in (presentation controller) in a protection (security) mode (col. 3, lines 27-33 and col. 8, lines 36-43). It can be selected that the images be changed to unprotected (col. 9, lines 5-8) which is interpreted by the examiner as placing the presentation controller in a by-pass mode.

As per claim 16, Schreiber et al teaches of a request blocker (data protector) that is coupled to the web browser (data handler) to prevent the providing of the protected data whereby the substitute pixel data replaces (by not providing) the protected pixel data (col. 4, lines 59-60 and col. 19, line 56). A modified layout page is presented to the user by using substitute data (delivering data other than the data requested) and not

delivering the original layout page containing the digital images to the requestor (col. 3, lines 39-47).

As per claim 17, it is disclosed by Schreiber et al of a system comprising a client computer that inherently contains a presentation circuit that is the hardware necessary to execute to the processing of the web browser presentation controller (col. 3, lines 40-47). A web browser (presentation controller) that transmits a request for data via a (output) port for presentation from a web page (col. 20, lines 25-27 and col. 22, lines 7-10). Also disclosed within the system is receiving data (via an input interface) in a video buffer (presentation buffer) that is associated with a web browser plug-in (presentation controller) that allows for displaying the image (col. 3, lines 27-33 and col. 4, lines 54-55). Contained within the system is a command processor (command handler) that processes commands made through the web browser to download information from web pages (located at a specific address)(col. 4, lines 54-60 and col. 6, lines 36-51). A web browser (additionally acting as a data handler) requests for data and pass the data to the video buffer (presentation buffer)(col. 3, lines 30-47). It is interpreted by the examiner that the web browser monitors for user requests to access data on the web pages (col. 6, lines 42-51). A request interceptor (security violation detector) detects requests by a client computer (requestor) to the protected data in the video buffer (presentation buffer)(col. 3, lines 39-47 and col. 6, lines 66-67). It is interpreted by the examiner that the data is then read by the user's computer since it is to be displayed to a user by means of the web browser plug-in (presentation controller)(col. 3, lines 27-33,39-47). A request blocker (data protector) that is coupled to the web browser (data

handler) to prevent the providing of the protected data whereby the substitute pixel data replaces (by not providing) the protected pixel data (col. 4, lines 59-60 and col. 19, line 56). Access is blocked to the pixel data of the digital image in the video buffer (presentation buffer)(col. 4, lines 37-42 and col. 18, lines 65-68).

As per claim 18, Schreiber et al teaches of a request blocker (data protector) that is coupled to the web browser (data handler) to prevent the providing of the protected data whereby the substitute pixel data replaces (purges) the protected pixel data (col. 4, lines 59-60 and col. 19, line 56). Data is received in a video buffer (presentation buffer) that is associated with a web browser plug-in (presentation controller) that allows for displaying the image (col. 3, lines 27-33 and col. 4, lines 54-55). It is interpreted by the examiner that the data is then read by the user's computer since it is to be displayed to a user by means of the web browser plug-in (presentation controller)(col. 3, lines 27-33,39-47).

As per claim 19, it is recited by Schreiber et al of a mode where protection applies on an image by image basis (col. 9, lines 1-4). The teachings disclose of the use of a video buffer (presentation buffer)(col. 3, lines 30-33) and it is inherent that a frame buffer is used since frame buffers hold the contents of a single screen image. The teachings also recite that the web browser plug-in (presentation controller) views images and is interpreted as being a graphics controller since the graphics are displayed on a video monitor (col. 6, lines 42-45).

As per claim 20, Schreiber et al discloses of placing the web browser plug-in (presentation controller) in a protection (security) mode (col. 3, lines 27-33 and col. 8,

lines 36-43). It can be selected that the images be changed to unprotected (col. 9, lines 5-8) which is interpreted by the examiner as placing the presentation controller in a by-pass mode.

As per claim 21, Schreiber et al teaches of a request blocker (data protector) that is coupled to the web browser (data handler) to prevent the providing of the protected data whereby the substitute pixel data replaces (purges) the protected pixel data (col. 4, lines 59-60 and col. 19, line 56). Data is received in a video buffer (presentation buffer) that is associated with a web browser plug-in (presentation controller) that allows for displaying the image (col. 3, lines 27-33 and col. 4, lines 54-55). It is interpreted by the examiner that the data is then read by the user's computer since it is to be displayed to a user by means of the web browser plug-in (presentation controller)(col. 3, lines 27-33,39-47). It is additionally recited by Schreiber et al of placing the web browser plug-in (presentation controller) in a protection (security) mode (col. 3, lines 27-33 and col. 8, lines 36-43). It can be selected that the images be changed to unprotected (col. 9, lines 5-8) which is interpreted by the examiner as placing the presentation controller in a by-pass mode.

As per claim 22, Schreiber et al teaches of a request blocker (data protector) that is coupled to the web browser (data handler) to prevent the providing of the protected data whereby the substitute pixel data replaces (by not providing) the protected pixel data (col. 4, lines 59-60 and col. 19, line 56). A modified layout page is presented to the user by using substitute data (delivering data other than the data requested) and not

delivering the original layout page containing the digital images to the requestor (col. 3, lines 39-47).

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Girard, US 2003/0005295 discloses of improving the protection of information presented by a computer.

Pizano et al, U.S. Patent 6,731,756 discloses of securing video images.

Schreiber et al, U.S. Patent 6,353,892 discloses of protection of digital images.

Schreiber et al, U.S. Patent 6,209,103 discloses of preventing the reuse of text, images, and software.

Lenehan et al, WO 02/25416 is a disclosure of the applicant's invention.

"SafeImage 1.34 Installation and Users Guide", general teaching for protecting view images.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 703-305-1843. The examiner can normally be reached on Monday-Friday, 6:30am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christopher Revak
AU 2131
5/13/04

CR
May 13, 2004